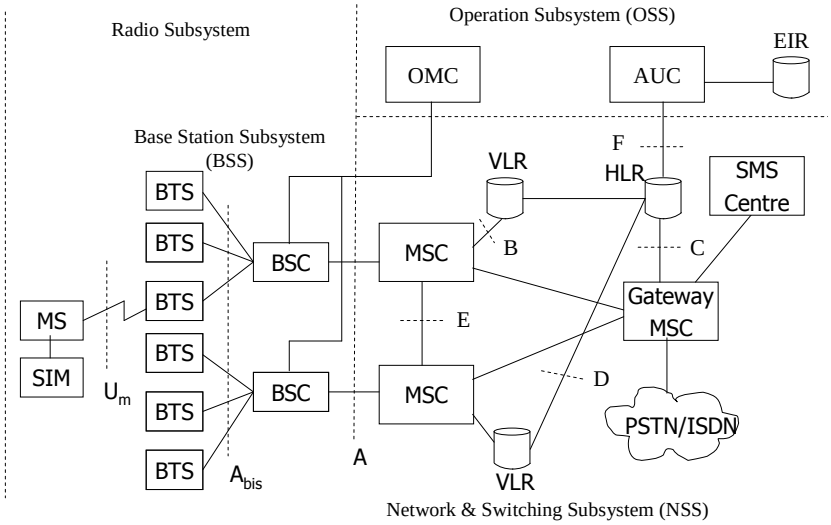
GSM Interfaces and Protocols

Telecommunications
MSc in Software Development

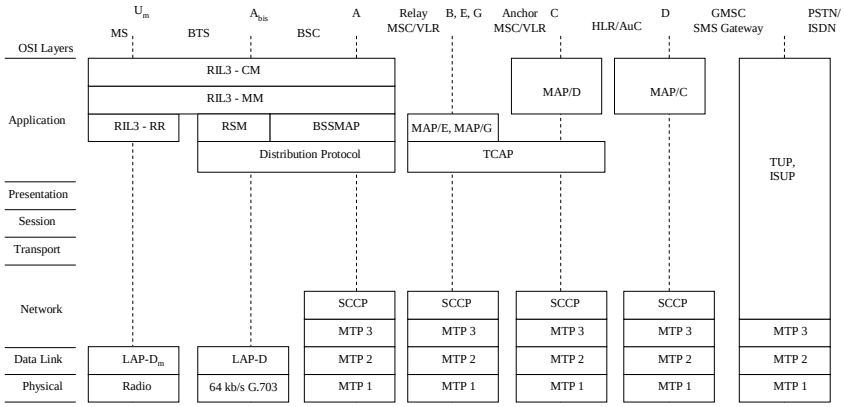
Introduction

- Communication between the several logical and physical entities of a GSM PLMN is based on specified interfaces and associated protocols
- Interfaces of radio access part
  - Radio Interface Um-Interface
  - BTS-BSC interface Abis-Interface
  - BSC-MSC interface A-Interface
  - NSS interfaces
    - B, C, D, E, F Interfaces

GSM Interfaces



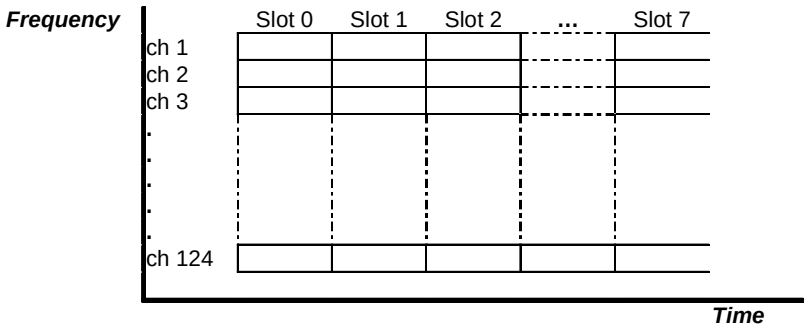
GSM Protocols



GSM Radio Interface

- Combination of FDM and TDM
- Uplink and downlink have each 25MHz of total spectrum available
- Spectrum divided into 124 carrier frequencies
- Carrier spacing is 200kHz
- 8 time slots per carrier

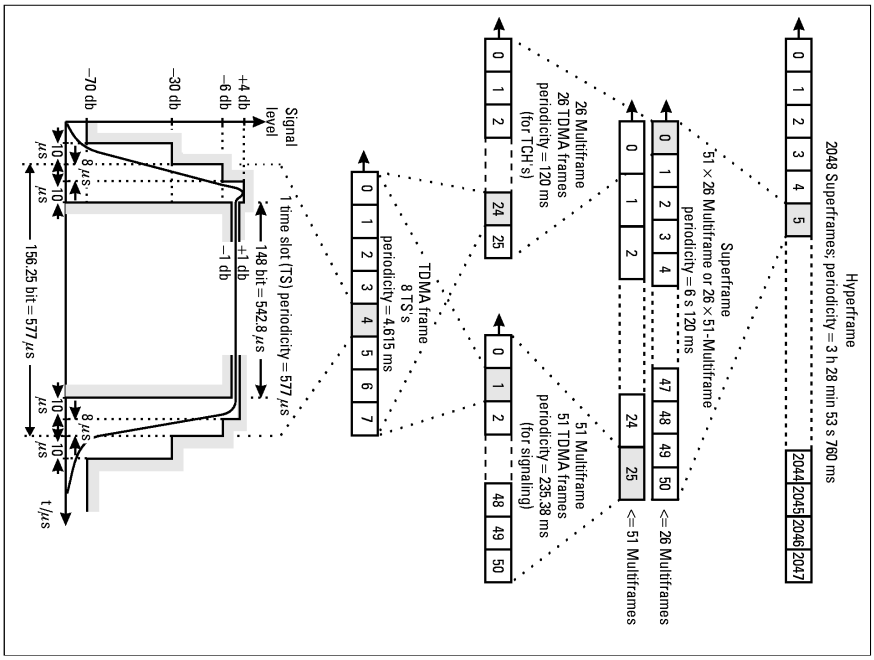
Multiplexing



1 Frame = 8 timeslots
Frame duration = 4.615 ms
timeslot duration = 0.577 ms

TDMA Frame Structure

- Each TDMA frame divided into 8 time slots
- TDMA frames are grouped into two types of multiframes
  - 26-frame multiframe for traffic channels
  - 51-frame multiframe for control channels
- Multiframes are multiplexed into single superframe of 6.12sec duration
- 2048 multiframes are combined into hyperframe


Hyperframe
2048 Superframes; periodicity = 3 h 28 min 53 s 760 ms
Superframe
51 × 26 Multiframe or 26 × 51-Multiframe
periodicity = 6 s 120 ms
<= 26 Multiframes
<= 51 Multiframes
26 Multiframe
26 TDMA frames
periodicity = 120 ms
(for TCH's)
51 Multiframe
51 TDMA frames
periodicity = 235.38 ms
(for signaling)
TDMA frame
8 TS's
periodicity = 4.615 ms
Signal level
+4 db
–6 db
–30 db
–70 db
–1 db
+1 db
1 time slot (TS) periodicity = 577 µs
148 bit = 542.8 µs
156.25 bit = 577 µs
8 µs
10 µs
t/µs

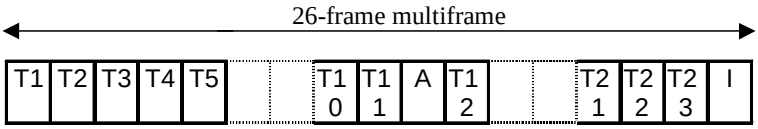
Channel Types

- Physical Channels
  - defined by carrier frequency/TDMA time slot combination
- Logical Channels
  - two types of logical channels
  - Traffic Channels (TCH)
  - Control Channels (CCH)

Traffic Channels

- Traffic channels carry user information
  - speech
  - data, FAX
- Two types of TCH
  - full rate channel with 22.8kbps gross bit rate
  - half rate channel with 11.4kbps gross bit rate
- TCH are multiplexed into 26-frame multiframe structure

26-frame Multiframe

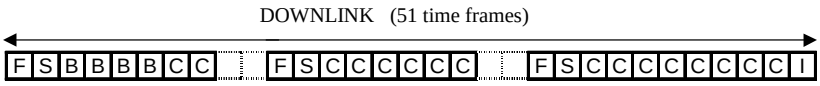


Tn: time frame number n for traffic data.
A: slow associated control channel.
I: idle frame.

Control Channels

- Control channels carry system control and synchronisation information
- Three categories are defined
  - Broadcast channel
  - Common control channel
  - Dedicated control channel
- Almost all control channels exist in the 51-frame multiframe structure

51-frame Multiframe



F: frequency correction channel
S: synchronisation channel
B: broadcast control channel
C: common control channel
I: idle frame

Broadcast Channel

- Frequency Correction Channel (FCCH)
- Synchronisation Channel (SCH)
- Broadcast Control Channel (BCCH)

Common Control Channel

- Paging Channel (PCH)
- Random Access Channel (RACH)
- Access Grant Channel (AGCH)
- Cell Broadcast Channel (CBCH)

Dedicated Control Channel

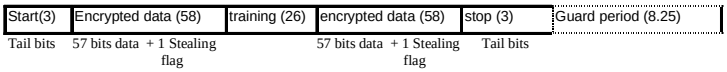
- Stand-alone Dedicated Control Channel (SDCCH)
- Slow Associated Control Channel (SACCH)
- Fast Associated Control Channel (FACCH)

Burst Types

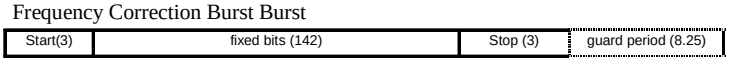
- Normal Burst
- Frequency Correction Burst
- Synchronisation Burst
- Dummy Burst
- Access Burst

Burst Types

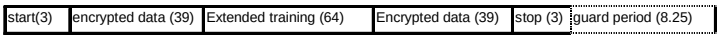
Normal Burst



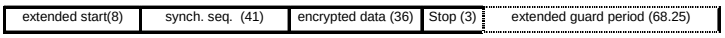
Frequency Correction Burst Burst



Synchronisation Burst



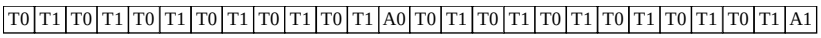
Access Burst



Channel Combinations

- CC1: TCH/F + FACCH/F + SACCH/TF
- CC2: TCH/H(0,1) + FACCH/H(0,1) + SACCH/TH(0,1)
- CC3: TCH/H(0) + FACCH/H(0) + SACCH/TH(0) + TCH/H(1)
- CC4: FCCH + SCH + BCCH + CCCH
- CC5: FCCH + SCH + BCCH + CCCH + SDCCH/4(0,1,2,3) + SACCH/C4(0,1,2,3)
- CC6: BCCH + CCCH
- CC7: SDCCH/8 + SACCH/8

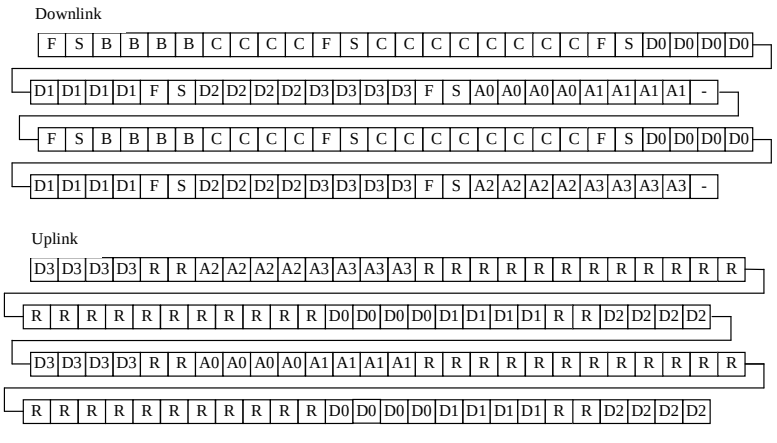
Channel Combination 2



T0: TCH/H(0) A0: SACCH/TH(0)
T1: TCH/H(1) A1: SACCH/TH(1)

26-frame multiframe

Channel Combination 5



F: FCCH D0: SDCCH/4(0) A0: SACCH/C4(0) R: RACH
F: FCCH D1: SDCCH/4(1) A1: SACCH/C4(1)
F: FCCH D2: SDCCH/4(2) A2: SACCH/C4(2)
F: FCCH D3: SDCCH/4(3) A3: SACCH/C4(3) 2 x 51-frame multiframe

CC based on Cell Load

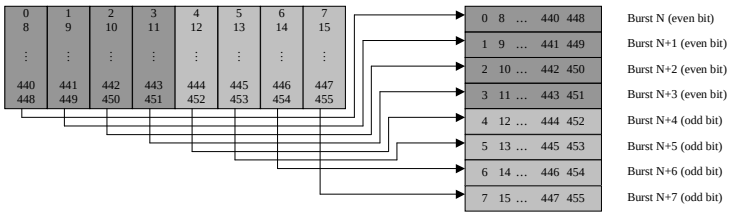
- **Low capacity cell with one TRX**
  - TN 0: FCCH + SCH + BCCH + CCCH + SDCCH/4(0,1,2,3) + SACCH/C4(0,1,2,3)
  - TN1 to TN7: TCH/F + FACCH/F + SACCH/TF
- **Medium capacity cell with four TRX**
  - Once (on TN 0): FCCH + SCH + BCCH + CCCH
  - Twice (on TN2 and TN4): SDCCH/8 + SACCH/8
  - 29 times: TCH/F + FACCH/F + SACCH/TF
- **High capacity cell with 12 TRXs**
  - Once on TN0: FCCH + SCH + BCCH + CCCH
  - Once on TN2: BCCH + CCCH
  - Once on TN4: BCCH + CCCH
  - Once on TN6: BCCH + CCCH
  - 5 times: SDCCH/8 + SACCH/8
  - 87 times: TCH/F + FACCH/F + SACCH/TF

1. Notice that a BCCH always appears in TN 0 together with the logical channels SCH and FCCH.
2. Additional combinations CC6 are added when traffic is expected to be heavy.

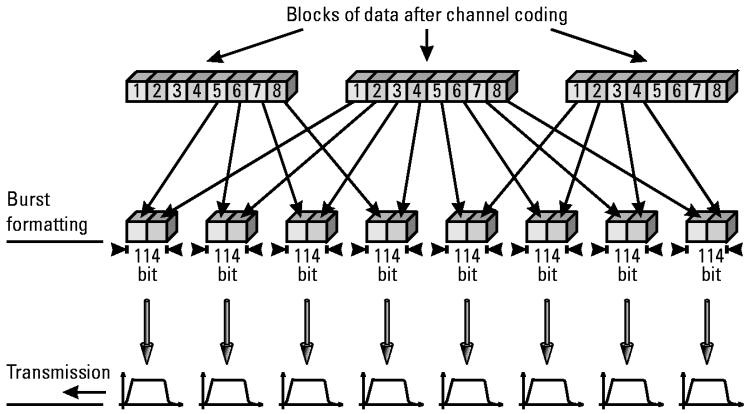
Channel Coding

- Block Code
  - Fire Code adds 40 bits redundancy, used on control channels
  - Generator polynomial $P(X) = (X^{23} + 1)(X^{17} + X^3 + 1)$
- Convolutional Code
  - coder rates of 1/2, 1/3, 1/6, and 244/456
- Interleaving

Interleaving



Interleaving

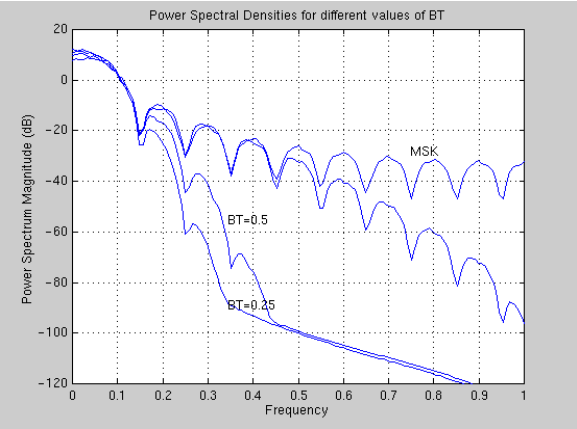


Coding on Logical Channels

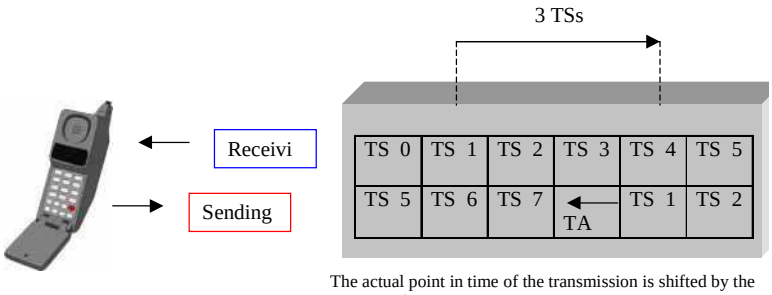
Channel Type	Bit/Block Data+Parity+Tail	Convolutional Coding Rate	Bit/ Block	Interleaving depth
TCH/FS			456	8
Class I	182 + 3 + 4	1/2	(378)	
Class II	78 + 0 + 0	-	(78)	
TCH/F9.6	4 * 60 + 0 + 4	244/456	456	19
TCH/F4.8	60 + 0 + 16	1/3	228	19
TCH/H4.8	4 * 60 + 0 + 4	244/456	456	19
TCH/F2.4	72 + 0 + 4	1/6	456	8
TCH/H2.4	72 + 0 + 4	1/3	228	19
FACCHs	184 + 40 + 4	1/2	456	8
SDCCHs, SACCHs	184 + 40 + 4	1/2	456	4
BCCH, AGCH, PCH	184 + 40 + 4	1/2	456	4
RACH	8 + 6 + 4	1/2	36	1
SCH	25 + 10 + 4	1/2	78	1

Modulation

- GMSK
- BT = 0.3



Timing Advance



The actual point in time of the transmission is shifted by the Timing Advance.

Signalling Application Protocols

- Radio Interface Layer (RIL) Protocols
  - Radio Resource (RR) Management
  - Mobility Management (MM)
  - Call Management (CM)
- BSS and NSS Protocols
  - Common Channel Signalling System #7 (CCS7)
  - TCAP
  - GSM MAP

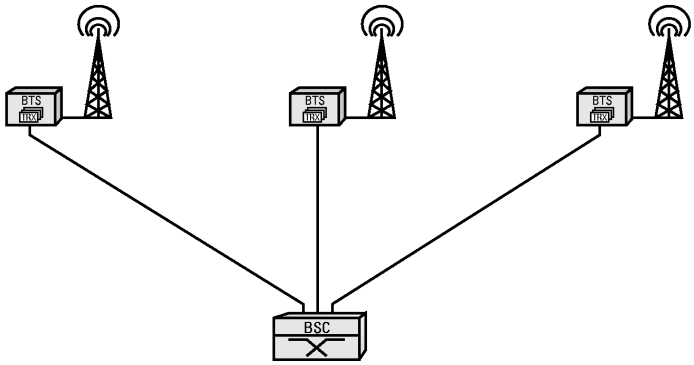
A_{bis}-Interface

- Interface between BTS and BSC
- Non-standardised interface, manufacturers follow certain guidelines
- Based on transmission of data on a PCM 30 interface (2.048Mb/s transmission rate partitioned into 32 channels of 64 kb/s each)
- Voice compression can pack between 4 and 8 voice channels into single PCM 30 channel.

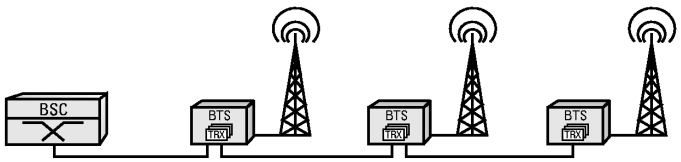
BSS Configurations

- Networking between BTSs and BSCs
- Multiplexing of user data
- Typical network configurations
  - Star Configuration
  - Ring Configuration
  - Serial Configuration

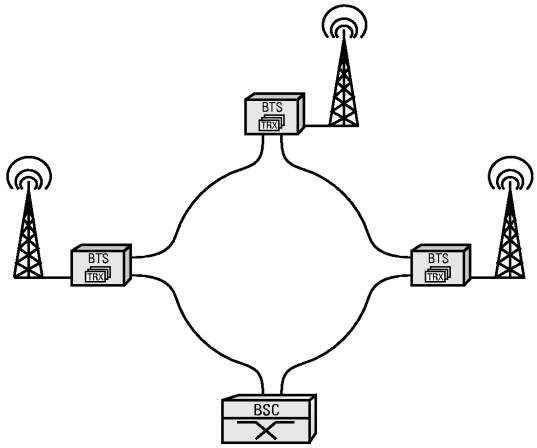
Star Configuration



Serial Configuration



Ring Configuration



Multiplexing - Star Configuration

0	FAS/NFAS					17	Not used
1	Air 0	Air 1	Air 2	Air 3	TRX 1	18	Not used
2	Air 4	Air 5	Air 6	Air 7		19	Partial O&M data
3	Air 0	Air 1	Air 2	Air 3	TRX 5	20	Not used
4	Air 4	Air 5	Air 6	Air 7		21	O&M signalling
5	Air 0	Air 1	Air 2	Air 3	TRX 2	22	TRX 8 signalling
6	Air 4	Air 5	Air 6	Air 7		23	TRX 7 signalling
7	Air 0	Air 1	Air 2	Air 3	TRX 6	24	TRX 6 signalling
8	Air 4	Air 5	Air 6	Air 7		25	TRX 5 signalling
9	Air 0	Air 1	Air 2	Air 3	TRX 3	26	Not used
10	Air 4	Air 5	Air 6	Air 7		27	TRX 4 signalling
11	Air 0	Air 1	Air 2	Air 3	TRX 7	28	TRX 3 signalling
12	Air 4	Air 5	Air 6	Air 7		29	TRX 2 signalling
13	Air 0	Air 1	Air 2	Air 3	TRX 4	30	TRX 1 signalling
14	Air 4	Air 5	Air 6	Air 7		31	Not used
15	Air 0	Air 1	Air 2	Air 3	TRX 8		
16	Air 4	Air 5	Air 6	Air 7			

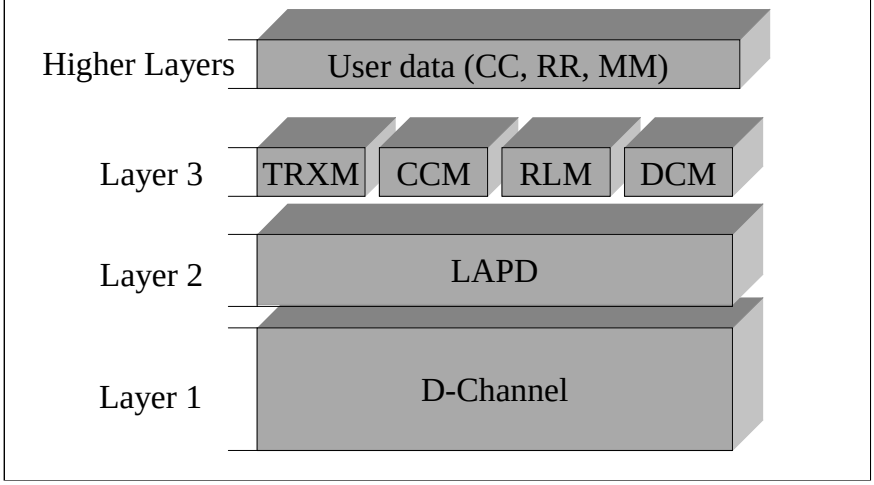
Multiplexing - Serial Configuration

0	FAS/NFAS					17	Not used	
1	Air 0	Air 1	Air 2	Air 3	BTS1/TRX1	18	Partial O&M data	
2	Air 4	Air 5	Air 6	Air 7		19	BTS4/TRX2 signalling	
3	Air 0	Air 1	Air 2	Air 3	BTS3/TRX1	20	BTS4/TRX1 signalling	
4	Air 4	Air 5	Air 6	Air 7		21	BTS3/TRX2 signalling	
5	Air 0	Air 1	Air 2	Air 3	BTS1/TRX2	22	BTS3/TRX1 signalling	
6	Air 4	Air 5	Air 6	Air 7		23	BTS2/TRX2 signalling	
7	Air 0	Air 1	Air 2	Air 3	BTS3/TRX2	24	BTS2/TRX1 signalling	
8	Air 4	Air 5	Air 6	Air 7		25	BTS1/TRX2 signalling	
9	Air 0	Air 1	Air 2	Air 3	BTS2/TRX1	26	BTS1/TRX1 signalling	
10	Air 4	Air 5	Air 6	Air 7		27	BTS4 O&M signalling	
11	Air 0	Air 1	Air 2	Air 3	BTS4/TRX1	28	BTS3 O&M signalling	
12	Air 4	Air 5	Air 6	Air 7		29	BTS2/O&M signalling	
13	Air 0	Air 1	Air 2	Air 3	BTS2/TRX2	30	BTS1/O&M signalling	
14	Air 4	Air 5	Air 6	Air 7		31	Transmission Control Information	
15	Air 0	Air 1	Air 2	Air 3	BTS4/TRX2			
16	Air 4	Air 5	Air 6	Air 7				

Control Signalling on the A_{bis}-Interface

- Layer 1 uses 64kb/s D-channel on E1 line (G.701/702) protocol
- Layer 2 uses the ISDN LAPD protocol
- Layer 3 divided into four parts
  - TRX Management (TRXM)
  - Common Channel Management (CCM)
  - Radio Link Management (RLM)
  - Dedicated Channel Management (DCM)

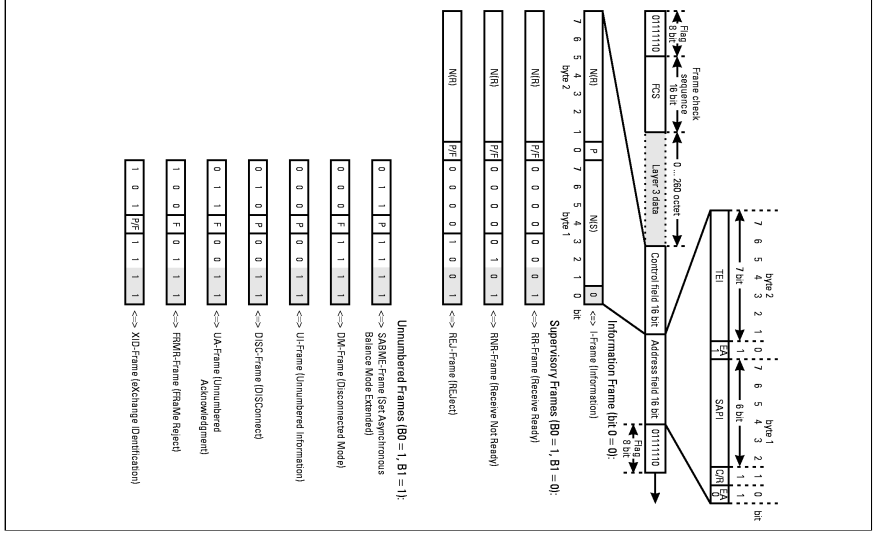
A_{bis}-Interface Protocol Stack



Layer 2 - LAPD

- GSM adopted basically ISDN layer 2 LAPD as defined in ITU recommendations Q.920 and Q.921
- Uses three frame types based on more general HDLC
  - Information frame group containing the I-frame
  - Supervisory frame group containing the RR, RNR, REJ frames
  - Unnumbered frame group containing the SABME, DM, UI, DISC, UA, FRMR, and XID frames
- Two protocol options based on window length of 8 and 128
  - GSM uses mainly the 128 window length option

LAPD Frame Format



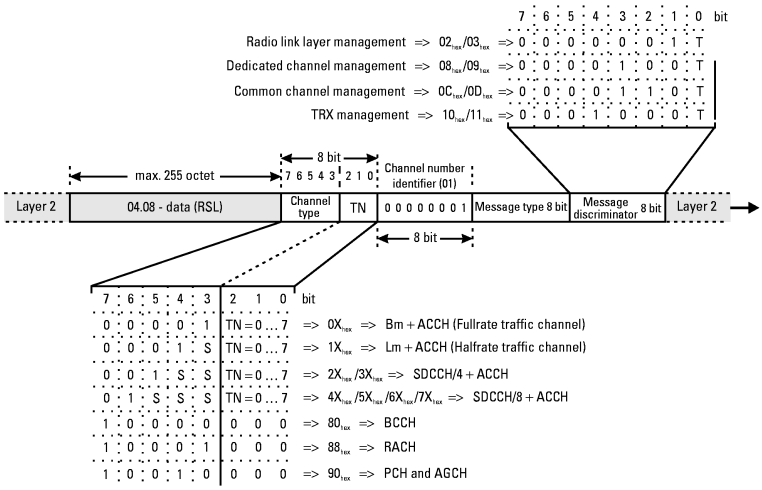
Layer 2 Addressing

- LAPD uses three SAPI (0, 62, and 63) to layer 3
  - SAPI 0 - radio signalling (radio signalling link, RSL)
    - connection setup, release
    - SMS and supplementary services messages
  - SAPI 62 - O&M messages (O&M link, OML)
  - SAPI 63 - Layer 2 management
  - SAPI 62 and 63 messages have priority so that during congestion the network can still be managed

Layer 3 Signalling

- Layer 3 consists of four parts
  - TRXM, CCM, DCM, RLM
- message transmission and format depends on SAPI
  - SAPI = 0 for radio link signalling, carries user data from CC, MM, RR, and also SMS and SS
  - SAPI = 62, 63 for OMC and layer 2 management.

Layer 3 RSL Message Format



Example Messages for RLM

ID (Hex)	Name	Direction	Description
01	DATA REQuest	BSC → BTS	Transport container for transparent transfer of BSSAP data from NSS to MS
02	DATA INDication	BTS → BSC	Transport container for transparent transfer of BSSAP data from MS to NSS
04	ESTablish REQuest	BSC → BTS	Request for BTS to establish layer 2 connection on radio interface.
05	ESTablish CONFirm	BTS → BSC	Answer to EST_REQ. Message sent to BSC after BTS receives an $LAPD_m$ UA frame from MS
06	ESTablish INDication	BTS → BSC	Response from BTS on receiving an $LAPD_m$ SABM frame from MS
07	RELease REQuest	BSC → BTS	Request to BTS to release current layer 2 connection. BTS sends an $LAPD_m$ DISC frame to MS.
0A	UNIT DATA REQuest	BSC → BTS	Transport frame to send messages sent in $LAPD_m$ UI frames over radio interface
0B	UNIT DATA INDication	BTS → BSC	Transport frame for messages received in $LAPD_m$ UI frames over radio interface

Example Messages for CCM and TRXM

ID (Hex)	Name	Direction	Description
11	BCCH INFOrmation	BSC → BTS	Transport frame for SYS_INFO messages for transmission in BCCH on time slot 0
12	CCCH LOAD INDication	BTS → BSC	Informs BSC about traffic load on CCCH of radio interface. Frequency of transmission may be adjusted by OMC.
13	CHANnel ReQuireD	BTS → BSC	Message sent by BTS on receipt of CHAN_REQ by MS.
15	PAGing CoMmanD	BSC → BTS	Response of the BSC on receipt of a PAGING command from MSC. Contains IMSI and/or TMSI and the paging group of called MS
16	IMMediate ASSign CoMmanD	BSC → BTS	Contains all information for assignment of a SDCCH on radio interface. Transmitted in response to receiving a correct CHAN_RQD.
19	RF RESource INDication	BTS → BSC	BTS uses this message to periodically inform BSC about quality and quantity of available resources on radio interface. Allows BSC to refrain from assigning channels with poor quality.
1C	ERROR REPORT	BTS → BSC	Used when error is detected by TRX and no other response message exists.

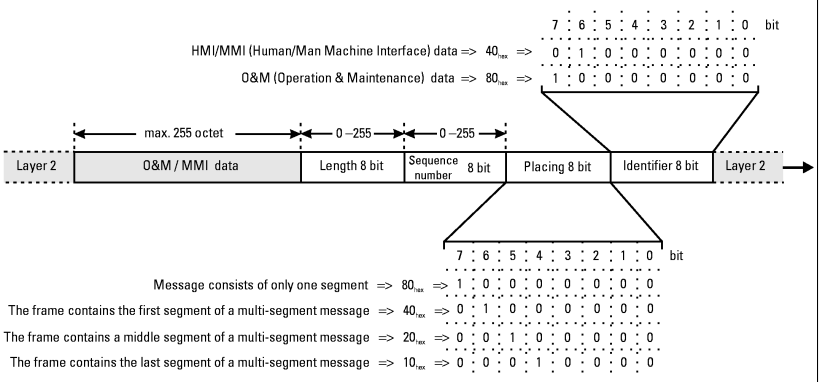
Example Messages for DCM

ID (Hex)	Name	Direction	Description
21	CHANnel ACTivation	BSC → BTS	Message to reserve and activate channels on the radio interface. Contains accurate description of requested channel (half/full rate, DTX on/off, channel type, etc.)
22	CHANnel ACTivation ACKnowledge	BTS → BSC	BTS acknowledges with this message reception of CHAN_ACT message and activation of requested channel.
24	CONNection FAILure	BTS → BSC	Message is sent in case of layer 1 problems on the radio interface
25	DEACTivate SACCH	BSC → BTS	Requests BTS to stop transmission over the SACCH. The DEACT_SACCH is part of the release procedure
26	ENCRyption CoMmanD	BSC → BTS	Activation of ciphering on the radio interface. Message contains the algorithm A5/X to be used.
27	HANDover DETect	BTS → BSC	HND_DET is used during handover (not for intra-BTS and intra-BSC handover). After target cell has received the HND_ACC message it calculates the distance to MS (TA) and sends result in HND_DET message to BSC. It also informs MSC about successful handover as soon as possible to allow for faster switching of the call.
28	MEASurement RESult	BTS → BSC	Contains the mutual measurement result of the MS and BTS.
2E	RF CHANnel RELease	BSC → BTS	RF_CHAN_REL message is sent to BTS after release of layer 2 connection to request release of layer 1 connection.
2F	MS POWER CONTROL	BSC → BTS	Message used by BSC to adjust the MS transmitter power according to current radio conditions
30	BS POWER CONTROL	BSC → BTS	Message used by BSC to adjust the BTS transmitter power according to current radio conditions

Layer 3 O&M Signalling

- Messages depend on individual equipment manufacturer
- Management messages as well as software updates and file transfer are included in signalling
- Message transfer distinguishes between O&M messages and HMI/MMI messages

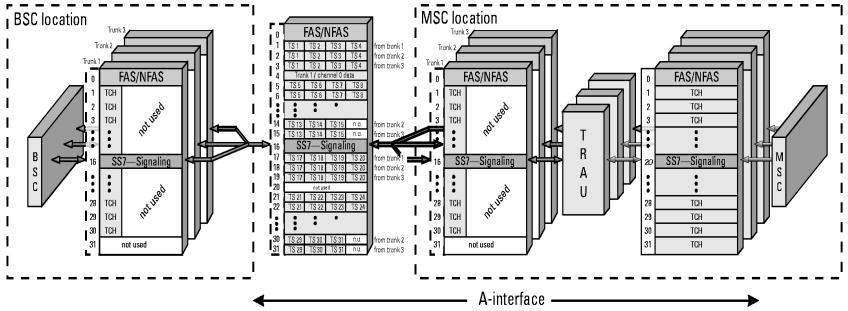
Layer 3 OML Message Format



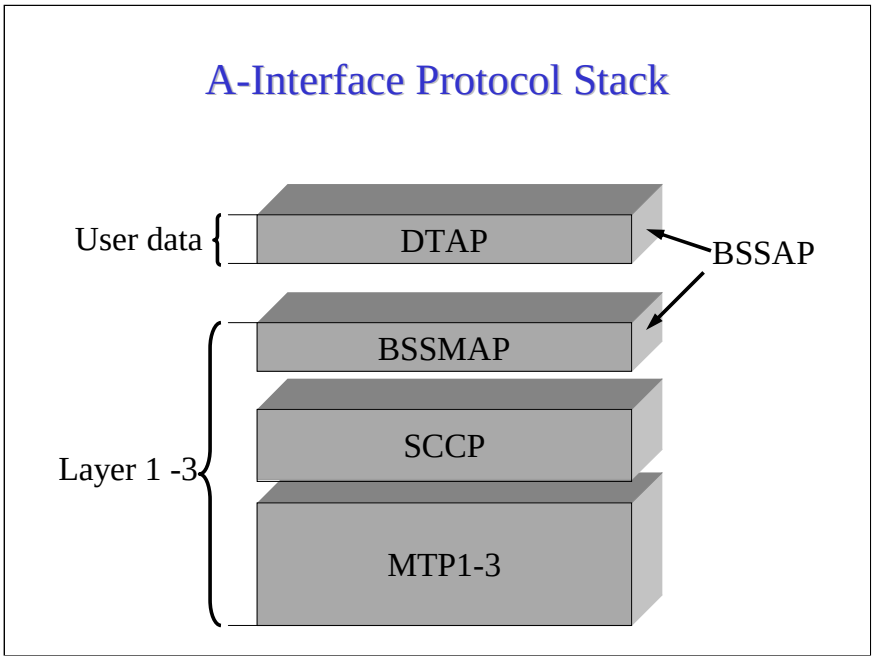
The GSM A-Interface

- Interface between BSS and MSC
- Standardised interface allows mixing of equipment from different manufacturers
- A-Interface at physical level consists of two parts
  - First part between BSS and TRAU, transmission payload is still compressed
  - Second part between TRAU and MSC
- A-Interface at higher layers depens on SS7 MTP and SCCP to carry BSSAP

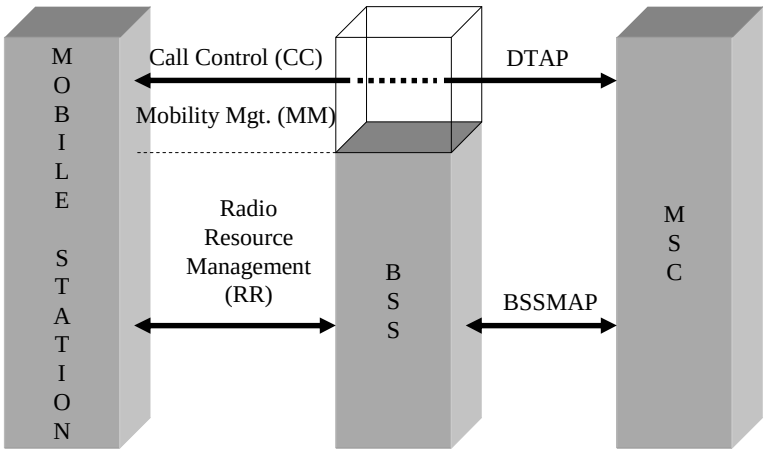
Multiplexing on A-Interface



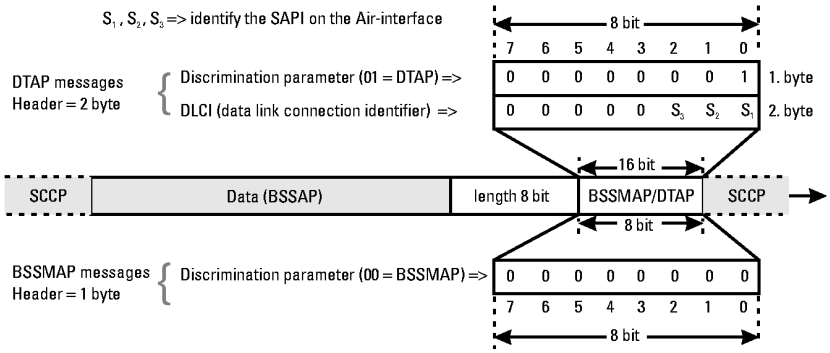
A-Interface Protocol Stack



A-Interface Message Relationships



Format of BSSAP Messages



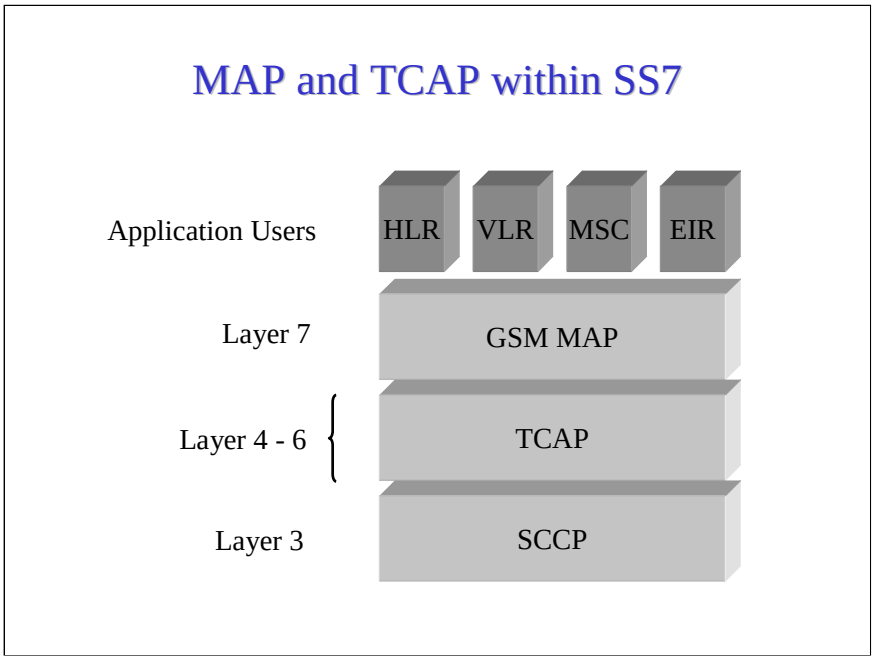
Example BSSMAP Messages

ID (Hex)	Name	Direction	Description
01	ASSignment REQuest	MSC → BSC	Sent from MSC to setup channel on radio interface and A-interface. BSC selects TCH out of list of available channels and assigns channel by means of ASS_CMD.
10	HaNDover REQuest	MSC → BSC	If the BSC needs to be changed during handover, this message is sent by the MSC to the new BSC.
11	HaNDover ReQuireD	BSC → MSC	BSC uses message to request handover from MSC (only intra-MSC and inter-MSC).
1B	HaNDover DETect	BSC → MSC	BSC reacts with this message when it receives a HND_DET message from the BTS on the Abis-interface.
20	CleaR CoMmanD	MSC → BSC	This message is always used to release the radio resources to a specific MS.
30	RESET	BSC ↔ MSC	In case of fatal errors with serious data incon-sistencies between MSC and BSC reset is performed. RESET message is used to synchronise BSC and MSC again. The message is also used when the A-interface is originally initialised
32	OVERLOAD	BSC ↔ MSC	Send to MSC in order to indicate overlaod situation in BTS or whole BSS. Possible to specify type of overload. MSC sends message to indicate processor overload in the switch.
34	RESet CIRCuit	BSC ↔ MSC	RES_CIRC is used like RESET. However, RES_CIRC only resets individual time slots on the A-interface rather than whole trunks.
40	BLOCK	BSC → MSC	Individual traffic channels need sometimes to be blocked for traffic.
50	RESource REQuest	MSC → BSC	MSC requests BSC with this message to provide updated information on the available radio resources of a BTS.
52	PAGING	MSC → BSC	In case of a mobile terminating call the MSC sends a PAGING message to all BSC of a location area.
53	CIPHER MODE CoMmanD	MSC → BSC	This message is sent in order to start ciphering on the radio interface.

GSM Mobile Application Part

- GSM uses the Mobile Application Part (MAP), a special application layer signalling protocol at all interfaces in the NSS
- MAP uses the SS7 protocol stack for message transmission between entities in the NSS
- MAP sits on top of SS7 TCAP and uses services of TCAP's structured dialogue for message transmission
- In typical applications MAP is often integrated with TCAP
- Dialogue between MAP applications starts with BEGIN and ends with END message

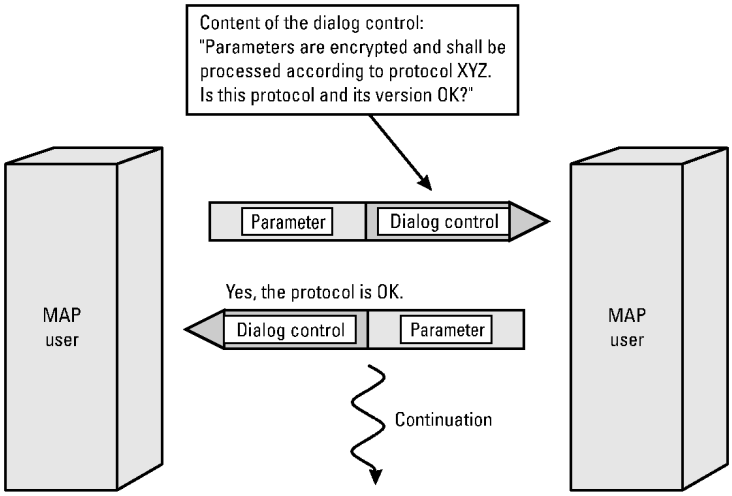
MAP and TCAP within SS7



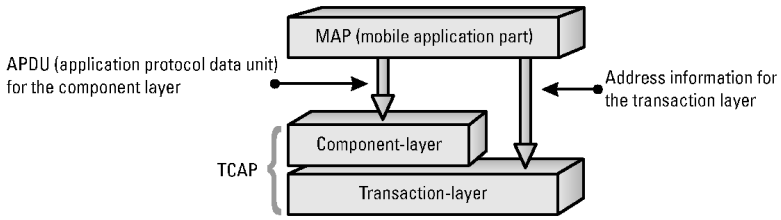
TCAP

- GSM TCAP uses exclusively the connectionless service of SCCP (protocol classes 0 and 1)
- Sending TCAP directly addresses the destination via the SCCP usually using the destinations global title (GT) address
- In GSM the global title is typically an entities ISDN number

Generic communication via TCAP



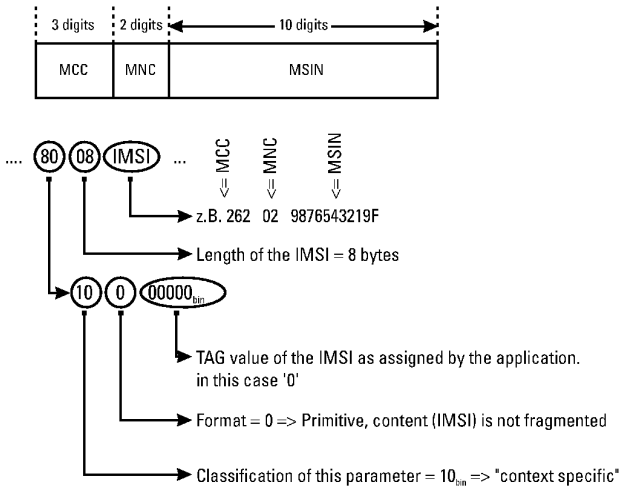
MAP and its relationship with TCAP's sublayers



Coding of Data in TCAP

- TCAP can encode length indicators from one byte to several thousand bytes
- Several parameter types are supported and encoding uses ASN.1 and associated encoding rules
- GSM uses the standard TCAP data encoding structure of three component elements (TLV convention)
  - Identifier (Type) T
  - Length of Value L
  - Contents (Value) V

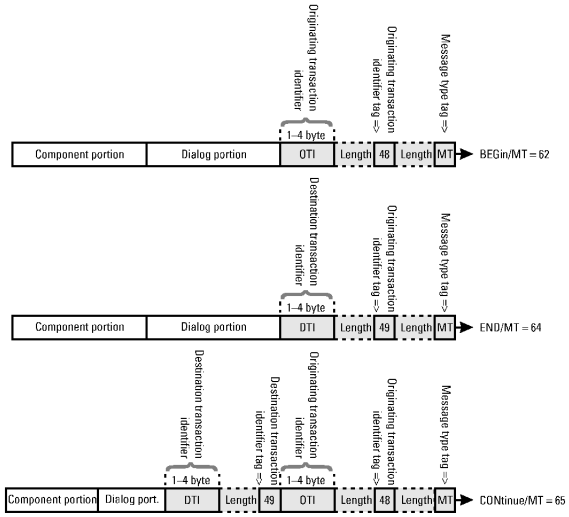
Example Coding of an IMSI in TCAP



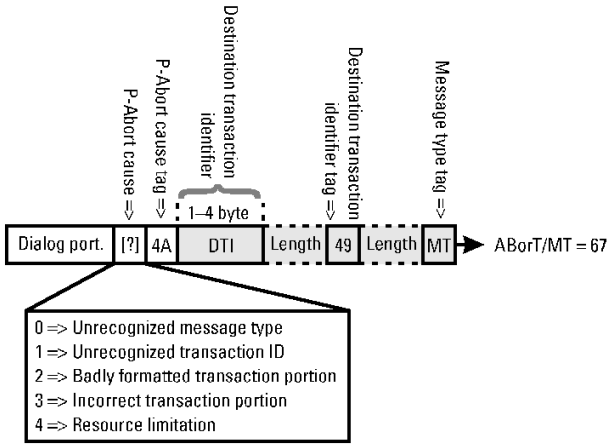
TCAP messages used in GSM

- Of the five defined TCAP messages, GSM uses only four
  - BEGin
    - Opens dialog for one user (MAP) to another user; comprises originating transaction ID.
  - END
    - Specifically ends a dialog process, which was started by BEG; may contain an optional component part with MAP data
  - CONtinue
    - Used between BEG and END to transport data; comprises of both originating and destination transaction ID; first CON after BEG confirms that protocol and context are ok.
  - ABorT
    - Both TCAP and MAP may use ABT to abort process if error or processing difficulty; reason may be provided; distinction is made between user and provider (U-ABORT and P-ABORT)

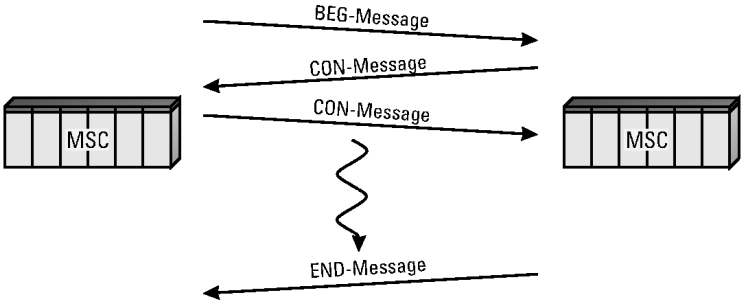
Structure of TCAP messages



Structure of TCAP messages



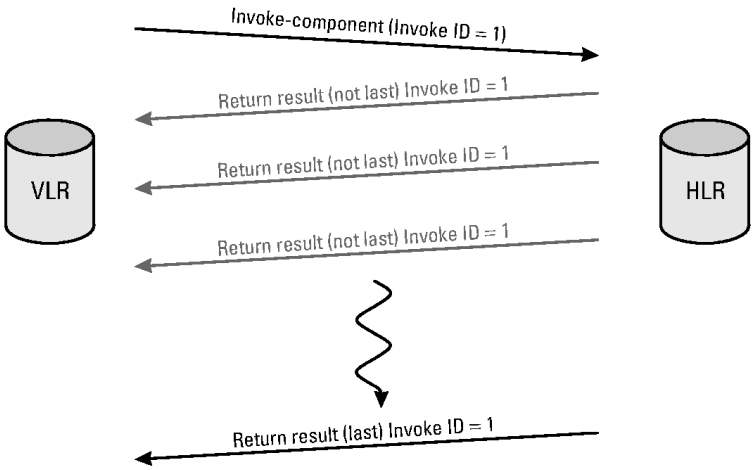
Structured Dialog in MSC-to-MSC Transaction



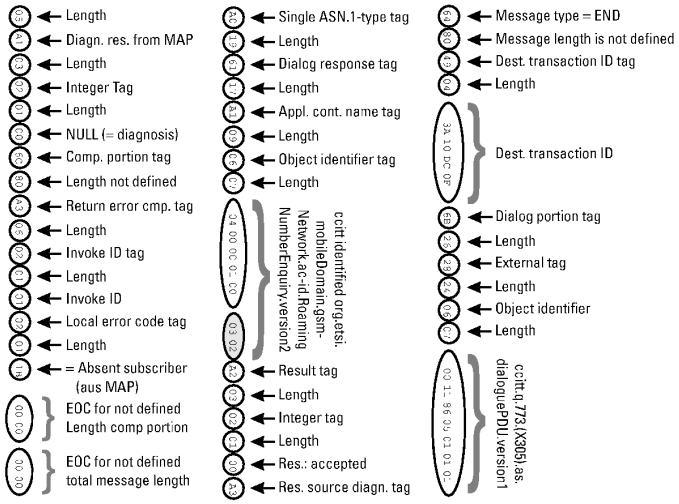
Component Portion

- The component portion is optional, but if present, contains user data
  - INVOKE Component
  - RETURN RESULT Component
  - RETURN ERROR Component
  - REJECT Component

Example use of *return result* Component



Decoding of an END Message



Decoded END Message

In plain text:

```
END
  Destination Transaction ID (hex) : 3A 10 DC 0F
  Dialogue Portion
    Protocol : {ccitt.Q.773.as.dialoguePDU.version1}
    Dialogue Response
      Application Context Name : {ccitt-ident-org.etsi.mobileDomain.gsm-Network
      ac-id.RoamingNumberEnquiry.version2}
      Result : 0 = accepted
      Result-Source-Diagnostic
        dialogue-service-user : 0 = null
  Component
    Return Error
      Invoke ID : 1
      Error Code
        Local Value : 27 = Absent Subscriber
```

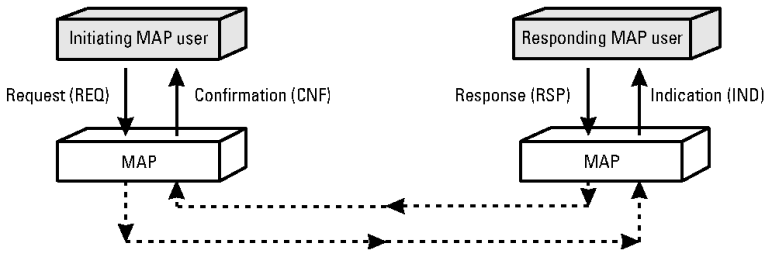
MAP Services

- MAP used to control communication between signalling application users such as HLR, VLR, and MSC
- MAP offers the following services
  - MAP-DELIMITER service
  - MAP-OPEN service
  - MAP-CLOSE service
  - MAP-U-ABORT service
  - MAP-P-ABORT service
  - MAP-NOTICE service

Special MAP Services

- Special MAP services (local operation codes in GSM terminology) define the actual type of data exchange between MAP users
- Examples
  - updateLocation
  - cancelLocation
  - registerSS
  - eraseSS
  - sendRoutingInfo
  - prepareHandover

Direction of MAP Services



Interaction between MAP and TCAP